

United States District Court

for the
Western District of New York



United States of America

v.

Case No. 23-MJ-

5098

TERRANCE MICHAEL CISZEK, a/k/a DrMonster

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about March 19, 2020, the exact date being unknown, in the Western District of New York, and elsewhere, the defendant, TERRANCE MICHAEL CISZEK, a/k/a DrMonster, knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, as defined in Title 18, United States Code, Section 1029(e)(3), that is, stolen login credentials, said possession affecting interstate and foreign commerce in that the defendant purchased the unauthorized access devices from a website based outside the United States.

All in violation of Title 18, United States Code, Section 1029(a)(3).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature

BRYAN SCHEIBER
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Printed name and title

Sworn to before me and signed telephonically.

Date: April 27, 2023

Judge's signature

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Bryan Scheiber, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint charging **TERRANCE MICHAEL CISZEK** (hereinafter “CISZEK”), with violations of Title 18, United States Code, Section 1029(a)(3) (knowingly and with intent to defraud, possessing fifteen or more devices which are counterfeit or unauthorized access devices).

2. I am a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”), and have been so employed since June 2021. I am currently assigned to the FBI Buffalo Field Office Cyber Task Force in Buffalo, New York, where I work on investigations relating to criminal and national security cyber intrusions. I received my Bachelor’s and Master’s degrees in Computer Science, have a Graduate Certificate in Computer Security and Information Assurance and hold several private sector computer security certifications. Prior to becoming an FBI Special Agent, I was a Computer Scientist with the FBI’s Washington Field Office. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

3. The facts set forth are based upon my personal observations, my training and experience, and information obtained during the course of the investigation from other members of law enforcement, involving the review of records, interviews of witnesses, and information

and reports provided. Because this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a Criminal Complaint and Arrest Warrant, I have not included each and every fact known by the government for this investigation.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

4. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market. Genesis Market is primarily hosted at the Internet domain “genesis.market.”¹ Genesis Market’s operators compile stolen data (*e.g.*, computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected² computers around the globe and package it for sale on the market.³ Genesis Market has been the

¹ A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website “g3n3sis.org,” as well as the TOR domain “genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxistepx2qd.onion.” TOR is short for “The Onion Router” and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user’s actual IP address, which could otherwise be used to identify a user.

² Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

³ Genesis Market refers to these packages of stolen data as “bots” on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market’s use of the word “bot” strays from the normal meaning, the term “package” is used throughout this request.

subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.⁴

5. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts (“resources”) associated with the package (*e.g.*, accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a “fingerprint” associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (*i.e.*, an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser’s ability to control and access the package’s data and masquerade as the victim device.

6. Genesis Market’s operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting

⁴ See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at <https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/> (last visited March 13, 2023).

packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

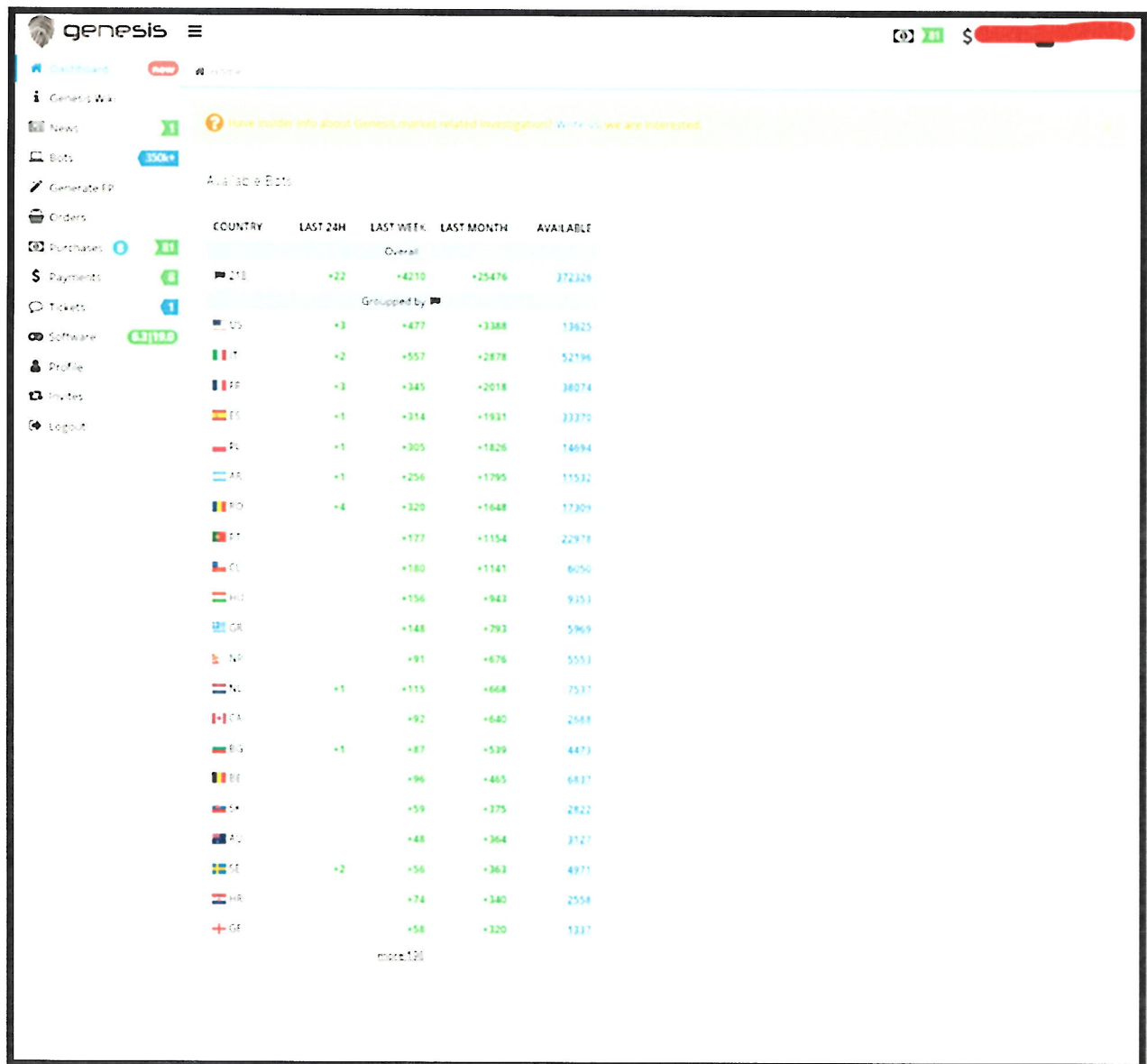
7. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then requests the new user to associate their Jabber ID⁵ or email address with that new account. Analysis by law enforcement has found that a Jabber ID or email address is not absolutely required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

8. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a “dashboard” of information, including the number of packages listed for sale and a “Genesis Wiki” page that walks a new user through Genesis Market’s platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.⁶ The front page displays the total

⁵ Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

⁶ Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

amount of “bots” (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

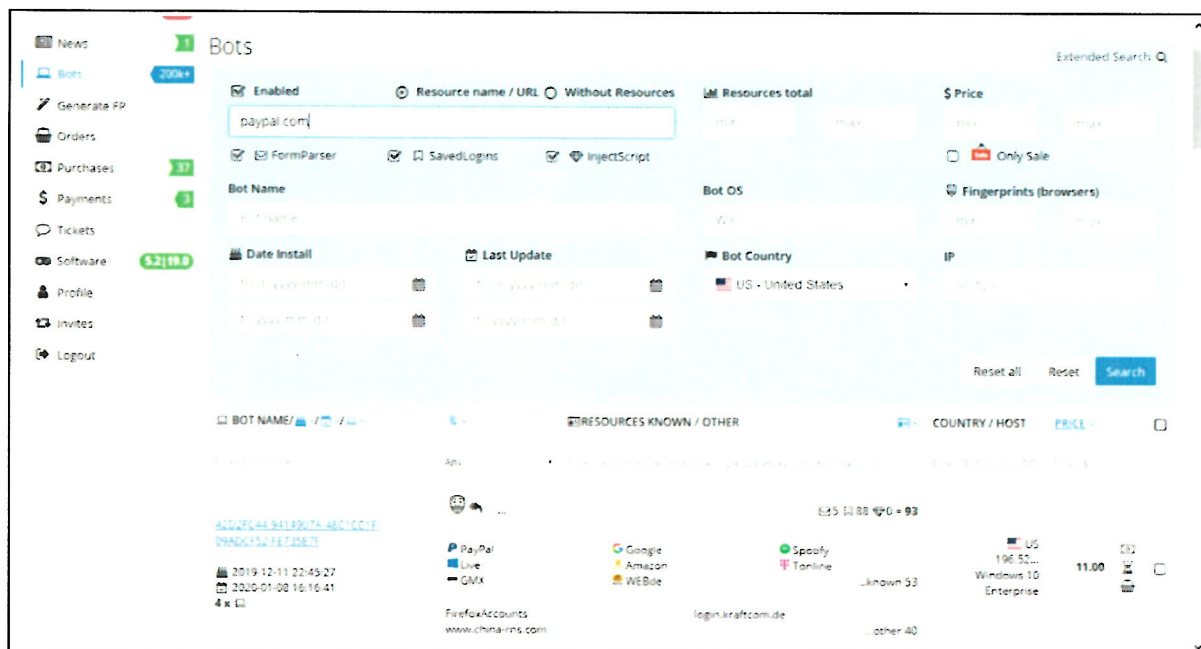


The screenshot shows the Genesis Market dashboard. On the left is a sidebar with navigation tabs: Dashboard, Genesis Wallet, News, Bots (350k+), Generate FP, Orders, Purchases (0), Payments (0), Tickets (1), Software (63/180), Profile, Invites, and Logout. The main content area is titled 'Available Bots' and features a table with columns: COUNTRY, LAST 24H, LAST WEEK, LAST MONTH, and AVAILABLE. The table is divided into an 'Overall' section and a 'Grouped by' section. The 'Overall' section shows a total of 372,328 available bots. The 'Grouped by' section lists 21 countries with their respective bot counts for the last 24 hours, last week, last month, and total available.

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
210	+22	+4210	+25476	372328
Grouped by				
US	+3	+477	+3388	13625
IT	+2	+557	+2878	52196
FR	+3	+345	+2018	38074
ES	+1	+314	+1931	33370
PL	+1	+305	+1826	14694
AR	+1	+256	+1795	11532
RO	+4	+320	+1648	17309
PT		+177	+1154	22978
CL		+180	+1141	6050
HU		+156	+943	9353
GR		+148	+793	5969
NP		+91	+676	5553
NO	+1	+115	+668	7537
CA		+92	+640	2583
BR	+1	+87	+539	4473
BE		+96	+465	6837
UA		+59	+375	2822
RU		+48	+364	3127
SE	+2	+56	+363	4971
HR		+74	+340	2558
GE		+58	+320	1337

more 100





9. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (*e.g.*, banking information, social media accounts, etc.), country of origin, price, and the date of infection (*i.e.*, the date the victim device was infected with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:



10. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee's purchase of a Genesis Market package:

7

Last update Saved Logins: 2019-11-22 08:55:29
 Last update Form Parser: 1970-01-01 00:00:00
 Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL / LOGIN / PASSWORD / ...	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
http://www.viewfabrics.com/register	SA	APN	SA	SA	
*Login: [REDACTED]@gmail.com *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
 Sony Entertainment Network https://accounts.sonyentertainmentnetwork.com/	SA	APN	SA	SA	
*Login: [REDACTED]@gmail.com *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
https://www.whiteboxlearning.com/login	SA	APN	SA	SA	
*Login: [REDACTED] *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
 Amazon https://www.amazon.com/ap/signin	SA	APN	SA	SA	
*Login: [REDACTED]@gmail.com *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
https://www.robox.com/	SA	APN	SA	SA	
*Login: [REDACTED] *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
 Google https://accounts.google.com/signin2?...	SA	APN	SA	SA	
*Login: [REDACTED]@gmail.com *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EAC04293-E544B574-B4E249CA-23041EF8-5E465696					
 Live https://login.live.com/oauth2/authorize?...	SA	APN	SA	SA	
*Login: [REDACTED]@gmail.com *Password: [REDACTED]	SA Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29

12. When users have questions or issues with Genesis Market, they can submit “tickets” via a “Ticket” tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

13. Purchases made through Genesis Market are conducted using digital currency, such as bitcoin.⁷ Before a purchase can be made, however, the user must first deposit a sum of digital currency into their Genesis Market account. This is done through the “Payments” tab on the Genesis Market website, wherein the user can choose the type of digital currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.⁸ Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

14. As of October 17, 2022, there were approximately 450,000 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device. According to Genesis Market’s website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

⁷ Digital currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Digital currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known digital currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

⁸ Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, the identity of which is known to law enforcement and known to be associated with criminal activity, to process the digital currency transactions.

15. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market. Through these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market operators through the “Ticket” function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims’ personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

16. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database A”). The database included, among other things, Genesis Market’s administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

17. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

18. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

19. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database B”). The database included the same types of information described above, including information from more than 55,000 Genesis Market user accounts.

Summary of Probable Cause Related to CISZEK

20. Genesis Market data showed that a Genesis user named Drmonster funded their account with cryptocurrency transactions. As described below, those transactions were traced to CISZEK. Based on that information, the FBI sought and obtained a federal search warrant for CISZEK’s residence. As described in more detail below, that search revealed evidence on CISZEK’s electronic devices of, among other things: (1) Genesis Market activity; (2) the purchase of stolen credit cards; and (3) online orders shipped to CISZEK’s premises with names other than CISZEK’s.

Drmonster’s Activity on Genesis Market

21. The Genesis Market data showed that, from March 16, 2020 to July 29, 2020, a user whose account name was Drmonster (“DRMONSTER”) purchased 11 packages on Genesis Market that included 194 stolen account credentials. The registration data for DRMONSTER showed the account was created on March 16, 2020, listed a Jabber ID of palatis3@gmail.com, and showed that DRMONSTER deposited \$80.36 to their marketplace account.

22. The Genesis Market data showed that DRMONSTER purchased the following packages on the marketplace⁹:

- a. PACKAGE 1, which included compromised credentials for victims' k12parent portal, Google, Twitter, Roblox, Target, and V3rmillion accounts.
- b. PACKAGE 2, which included compromised credentials for victims' Epic Games, Facebook, Sony Entertainment, Target, Discord, Twitch, Yahoo, and Microsoft Live accounts.
- c. PACKAGE 3, which included compromised credentials for victims' Target, Google, Apple, Steam, Grammarly, IXL, Recursive Arts, Tetris Friends, and Tetris Online accounts.
- d. PACKAGE 4, which included compromised credentials for a victim's UPS account.
- e. PACKAGE 5, which included compromised credentials for victims' Amazon and Microsoft Live accounts.
- f. PACKAGE 6, which included compromised credentials for victims' Freedom Mortgage, Brain Foresee, AT&T, Hot Mit, and Amazon accounts.
- g. PACKAGE 7, which included compromised credentials for victims' VPN service, Hulu, Local Government Solutions, Amazon, and Staples accounts.

⁹ As noted, DRMONSTER purchased 194 stolen credentials. This summary is therefore not an exclusive list of the credentials that DRMONSTER purchased.

- h. PACKAGE 8, which included compromised credentials for victims' Fanuc, Amazon, Facebook, Hulu, and Church of Jesus Christ accounts.
 - i. PACKAGE 9, which included compromised credentials for victims' Nextdoor, Amazon, North Providence (Rhode Island) Cloud, Smithfield (Rhode Island) Cloud, Microsoft Live, Zip Recruiter, Cox, MyKPlan, and Best Buy accounts.
 - j. PACKAGE 10, which included compromised credentials for victims' Google, PrivateVPN, Hulu, Amazon, Netflix, Free Hard Music, SoundPark Club, GMX email, MediaFire, pCloud, GloDLS, Walmart, eBay, Shentel, NexusMods, Steam, Fedex, SNaHP, UPS, Emuparadise, Ulozto, Roku, CloudMe, Nuts.com, PowerFolder, Rapidgator, Uploadrar, R1db, CoverCity, Canon, Torrenting, Dollar General, Kingdom Leaks, AllSync, Getspace, SugarSync, Zoho, Apple, DriveOnWeb, LinkedIn, Forge of Empires, OI Solutions, 500px, KatFile, Icedrive, Cloudup, ImageShack, TehParadox.Net, CoffeeCup, Facebook, Metal Tracker, 4shared.com, Autodesk, Uptobox, FilePup, FlipDrive, IDrive, Jottacloud, Keep2Share, Oboom, HiDrive, AnonFile, Twitter, SendSpace, FileCat, Spotify, and Android-Zone accounts.
 - k. PACKAGE 11, which included compromised credentials for victims' Gestione email, Cron Online, Randstad, Usborne Books, Facebook, Grenke, Rivenditori Lottomatica, Sky, Pedemontana, Greetings Island, Cartucce, Ferrero, Amazon, Spaggiari, and Scarm accounts.
23. Genesis Market data showed that DRMONSTER accessed the marketplace multiple times from the IP address 67.252.42.6 between March 16, 2020 and March 29, 2020 and

accessed the marketplace from the IP address 67.252.37.144 once on April 21, 2020. Open source research found the IP addresses 67.252.42.6 and 67.252.37.144 were registered to Charter Communications Inc. and were geolocated to Buffalo, New York.

24. On January 10, 2023, the FBI conducted open source research on the email address palatis3@gmail.com and found a LinkedIn account for CISZEK that identified CISZEK as a student at Erie Community College from 2008 to 2011. CISZEK is a detective with the Buffalo Police Department, in Buffalo, New York, and has been a law enforcement officer since January 2014.

25. On or about January 20, 2023, Google responded to legal process for the Google Account palatis3@gmail.com. Google's records identified CISZEK as the account owner and showed that the account was accessed multiple times between April 21, 2022 and July 28, 2022 from the IP address 67.252.37.144. Google did not provide IP address information further back than April 21, 2022 for the account.

26. On or about February 22, 2023, Charter Communications Inc. responded to legal process for the IP address 67.252.37.144 for the timestamp July 28, 2022 at 10:18 AM GMT, an instance where the IP address 67.252.37.144 had accessed the Google Account palatis3@gmail.com. Investigators chose the date of July 28, 2022, rather than a date that corresponds with activity on Genesis, because, based on my training and experience, I know that most Internet Service Providers (ISPs), such as Charter Communications Inc., retain IP address logs for between six to twelve months. Charter Communications Inc.'s records showed the IP address 67.252.37.144 was assigned to CISZEK at the service address 326 GRANT ST, UPPR,

BUFFALO, NY 142131422 (the PREMISES) with a lease log start date of September 13, 2021 and lease log end date of November 4, 2022.

27. On or about February 22, 2023, a Privacy Specialist with Charter Communications Inc. told the FBI that the subscriber for IP address 67.252.37.144 could have been assigned the IP address prior to that lease period. Based upon my training and experience, I know that most residential Internet Service Providers (“ISP”), such as Charter Communications, retain IP address logs for between six to twelve months and may continue to assign the same IP address to a subscriber while the subscriber’s internet router or modem remains online.

Cryptocurrency Tracing Related to DRMONSTER’s Genesis Purchases

28. DRMONSTER funded their Genesis Market account through two bitcoin transactions: Transaction 1 on March 19, 2020 for 0.005566 bitcoin with the transaction hash 788e2cef8a80f83bd190fef5e1c2c8ee3a113110c8dae9b667a7bbcb0daafc6e and Transaction 2 on March 19, 2020 for 0.007974 bitcoin with the transaction hash 2e53940298967c4d98a0f4bc235ad1b66a0635cd3a738c2ea548e7af71fef102. Investigators conducted cryptocurrency tracing and found that TRANSACTION 1 and TRANSACTION 2 originated from a cryptocurrency exchange named Block, Inc.

29. TRANSACTION 1, with the transaction hash 788e2cef8a80f83bd190fef5e1c2c8ee3a113110c8dae9b667a7bbcb0daafc6e, originated from the bitcoin wallet address 1FUEuXzfrYR3gobs7Hf1JFkRL4ZCpBdWen. Bitcoin wallet address 1FUEuXzfrYR3gobs7Hf1JFkRL4ZCpBdWen had only two transactions: the outbound transaction to Genesis Market and an inbound bitcoin transaction in the transaction hash

2e2c4328817f3c1450aca6a40a7a0921765cefe07e90d96006bb6e532fc1fbf6 that was traced to the cryptocurrency exchange Block Inc.

30. TRANSACTION 2, with the transaction hash 2e53940298967c4d98a0f4bc235ad1b66a0635cd3a738c2ea548e7af71fef102, originated from the bitcoin wallet address 1NxS8A3zmYryNGLykBEmb4fpzDRNio7Qo8. Bitcoin wallet address 1NxS8A3zmYryNGLykBEmb4fpzDRNio7Qo8 had only two transactions: the outbound transaction to Genesis Market and an inbound bitcoin transaction in the transaction hash 61ac3bf00187b8a6cd5dcd1f541941036c7e679e536c2390f0873bd3ce2eec67 that was traced to the cryptocurrency exchange Block Inc.

31. In summary, the cryptocurrency tracing described above showed that DRMONSTER funded his Genesis purchases with bitcoin that was sent from, in two transactions, a Block Inc. account to two separate bitcoin wallets, before being used to fund Genesis purchases. Particularly because the pass-through wallets had no activity other than that described above, based on my training and experience, this activity is consistent with that of someone who is attempting to obfuscate the source of payments for illegal activity.

32. On February 22, 2023, Block Inc. responded to legal process for the bitcoin transaction hashes 2e2c4328817f3c1450aca6a40a7a0921765cefe07e90d96006bb6e532fc1fbf6 (associated with TRANSACTION 1) and 61ac3bf00187b8a6cd5dcd1f541941036c7e679e536c2390f0873bd3ce2eec67 (associated with TRANSACTION 2) and provided, for both transaction hashes, a single Block Inc. account for CISZEK that listed the customer's email address as palatis3@gmail.com. Review of the Block Inc. account's bitcoin transactions found transactions associated with both transaction hashes

2e2c4328817f3c1450aca6a40a7a0921765cefe07e90d96006bb6e532fc1fbf6 and 61ac3bf00187b8a6cd5dcd1f541941036c7e679e536c2390f0873bd3ce2cec67 were sent from CISZEK's account. Block Inc. provided "know your customer" (KYC) information for CISZEK's Block Inc. account, which included a photograph of CISZEK's New York State Driver License.

33. Block Inc. provided IP addresses that accessed CISZEK's Block Inc. account. On March 16, 2020 at 18:24:11 UTC, CISZEK's Block Inc. account was accessed from the IP address 67.252.42.6. As noted above, DRMONSTER registered their Genesis Market account from the IP address 67.252.42.6 on March 16, 2020 at 18:43:14 (timezone unknown).

34. In summary, the above paragraphs show there is probable cause to believe that CISZEK's Block Inc. account funded DRMONSTER's Genesis Market account, which was then used to purchase 11 packages that included 194 stolen account credentials.

35. During the course of the investigation, investigators learned the email address palatis3@gmail.com may also be associated with a Coinbase account. Coinbase is a digital currency exchange similar in functionality to Block Inc.

36. On January 23, 2023, Coinbase responded to legal process for the email address palatis3@gmail.com and provided records for a Coinbase account that listed CISZEK as the owner. Coinbase included KYC information for CISZEK's Coinbase account, to include a New York State Driver License for CISZEK, that listed the PREMISES, and CISZEK's City of Buffalo Police Department identification card.

37. Coinbase's records showed that on April 13, 2020, CISZEK's Coinbase account sent 0.02697099 bitcoin to a bitcoin wallet address whose subsequent outbound transfers were

limited to bitcoin wallet addresses associated with UniCC and LuxSocks.ru. UniCC was a dark web carding website that announced its closure around January 2022. Carding websites are illicit marketplaces and/or forums used to share stolen credit card data and discuss techniques for obtaining credit card data, validating it and using it for criminal activity. UniCC was affiliated with LuxSocks.ru, a dark web residential proxy service that also closed during the same time period as UniCC.¹⁰

Search Warrant for 326 Grant Street

38. Based on the facts set forth above, on April 3, 2023, the Honorable Michael J. Roemer, U.S. Magistrate Judge of the United States District Court for the Western District of New York, signed a federal search warrant for CISZEK and the PREMISES.

39. On April 4, 2023, the FBI executed the aforementioned search warrant at the PREMISES and seized multiple electronic devices, to include a Samsung Galaxy S7 Edge (“PHONE 1”), HP Envy Desktop PC (“COMPUTER 1”), a SanDisk 32 USB Thumbdrive (“USB DRIVE 1”) and a SanDisk Cruzer 64GB (“USB DRIVE 2”) from the PREMISES.

40. FBI agents interviewed CISZEK during the search on April 4, 2023. CISZEK told agents, among other things, that (1) he was not familiar with using the Tor Browser nor dark web marketplaces or forums; (2) he had no computer training; (3) he had three email addresses:

¹⁰ Residential proxy services route the user’s internet traffic through residential Internet Service Provider (“ISP”) IP addresses. From a website’s prospective, the traffic from a residential proxy service appears to originate from a residence rather than its original source. Residential proxy services are often marketed to people seeking the ability to evade country-specific blocking by media streaming providers, but based on my training and experience, are also abused by those engaged in cybercrime activity because their use will trace malicious traffic to an unsuspecting residence.

palatis3@gmail.com, palatis100@gmail.com, and buffalodetective@gmail.com and; (4) his nephew could have been responsible for some of the online purchase of stolen credentials from dark web sites which was the subject of the FBI's investigation.¹¹ CISZEK further claimed that he had never purchased stolen credentials online, had no knowledge of anyone doing so, and had never been hacked or the victim of fraud.

41. Investigators' analysis of electronic devices seized from the PREMISES found evidence that was inconsistent with some of the statements CISZEK made to agents on April 4, 2023.

42. Investigators found the Tor Browser software on COMPUTER 1 and USB DRIVE 1. Investigators also found the Tails operating system image on COMPUTER 1 and Tails installed to USB DRIVE 2.¹²

¹¹ For the reasons set forth in this affidavit, there is probable cause to believe that CISZEK's claim that his nephew could have been responsible for the activity described in this affidavit is false. Moreover, agents interviewed CISZEK's nephew on April 6, 2023. CISZEK's nephew denied making purchases on Genesis Market and told agents that while he did have a smartphone, he did not have a computer. User Agent Strings for DRMONSTER's activity on Genesis Market (which could be used to help identify the device that was used to access Genesis Market) were not available in the Genesis Market data. However, as described below, Genesis Market offered users with a proprietary web browser, named Genesium Browser. Genesium Browser was based on the Google Chromium web browser and was available for the MacOS, Windows and Linux operating systems, all of which must use a computer to operate. DRMONSTER downloaded the Genesium Browser for the Microsoft Windows operating system on four occasions between March 2020 and July 2020. Based on this fact, as well as my training and experience, I submit that there is probable cause to believe that DRMONSTER accessed Genesis using either a laptop or a personal computer. Both CISEZK's nephew, and the mother of CISZEK's nephew, told Agents that CISZEK's nephew has never owned a computer. Further, as described below, agents found the Genesium Browser on one of CISZEK's devices.

¹² Tails is a security-focused Linux operating system that connects to the Internet exclusively through the anonymity network Tor. The system is designed to be booted as a live DVD or live USB and leaves no digital footprint on the machine unless explicitly told to do so.

43. Investigators also found evidence on USB DRIVE 1 and COMPUTER 1 showing that those devices were used by CISZEK. For example, USB DRIVE 1 contained a rental agreement PDF document, dated February 4, 2020, between CISZEK and tenants for use of the dwelling located at 326 Grant St, Buffalo, NY 14213 Lower Apt. CISZEK was listed as the owner on the rental agreement.

44. In addition, USB DRIVE 1 and COMPUTER 1 stored a folder named “Spring 2010 ECC” with files that included a Microsoft Word file named “What is Law enforcement.doc” with CISZEK’s name, Student ID and a due date of February 5, 2020. As noted, a publicly-available online profile identified CISZEK as having attended Erie Community College (ECC) from 2008 to 2011.

Vimeo Video and Use of Apparent Victim Identities

45. As described below, when searching a cell phone seized from CISZEK’s home, investigators found a video narrated by CISZEK that described how to use various software programs; showed a “DRMONSTER.vdi” icon the desktop; and concluded with CISZEK stating that he usually got his credit cards from UniCC.

46. On April 5, 2023, investigators began to review PHONE 1 and found five Gmail email accounts, and their email messages, stored on PHONE 1. Identified email accounts did not include the three email accounts that CISZEK provided to interviewing FBI agents on April 4, 2023 but did include rainbowfishie55@gmail.com (“EMAIL ACCOUNT 1”) and EMAIL

ACCOUNT 2.¹³ EMAIL ACCOUNT 1 and EMAIL ACCOUNT 2 had emails from one of the email accounts that CISZEK stated he used.¹⁴ Those emails contained what appeared to be a bitcoin wallet address.

47. Email messages in EMAIL ACCOUNT 1 and EMAIL ACCOUNT 2, which were stored on PHONE 1, included order confirmation messages from online retailers followed shortly thereafter by payment declined email messages. The purported customer in these emails was someone other than CISZEK. However, the shipping address for most of the purchases was CISZEK's residence at 326 Grant Street.¹⁵

48. For example, on April 15, 2020, EMAIL ACCOUNT 1 received an email message from NewEgg.com that stated NewEgg received an order for an Acer Aspire 3 15.6" laptop computer with the shipping address listed as VICTIM 2 at 326 Grant Street, Buffalo, NY 14213-1422 and the billing address listed as VICTIM 2's actual billing address. On April 16, 2020, EMAIL ACCOUNT 1 received a second email message from NewEgg.com that stated NewEgg was unable to process the order because the payment authorization on their credit/debit card had been declined.

¹³ EMAIL ACCOUNT 2 was similar to VICTIM 1's name. VICTIM 1 told an FBI agent during a telephonic interview on April 11, 2023 that VICTIM 1 did not recognize EMAIL ACCOUNT 2 as an email address they had used.

¹⁴ Email address rainbowfishie55@gmail.com received an email from palatis3@gmail.com on April 14, 2020 that contained what appeared to be a bitcoin wallet address in the message body. EMAIL ACCOUNT 2 sent an email to palatis3@gmail.com on April 9, 2020 that contained what appeared to be a bitcoin wallet address in the message body.

¹⁵ Investigators identified one email that listed a shipping address of 324 Grant Street, which is next to 326 Grant Street.

49. EMAIL ACCOUNT 1 received an email message from Vimeo dated April 15, 2020 at approximately 11:21 PM welcoming them to Vimeo. Vimeo is a video sharing platform, similar to YouTube.

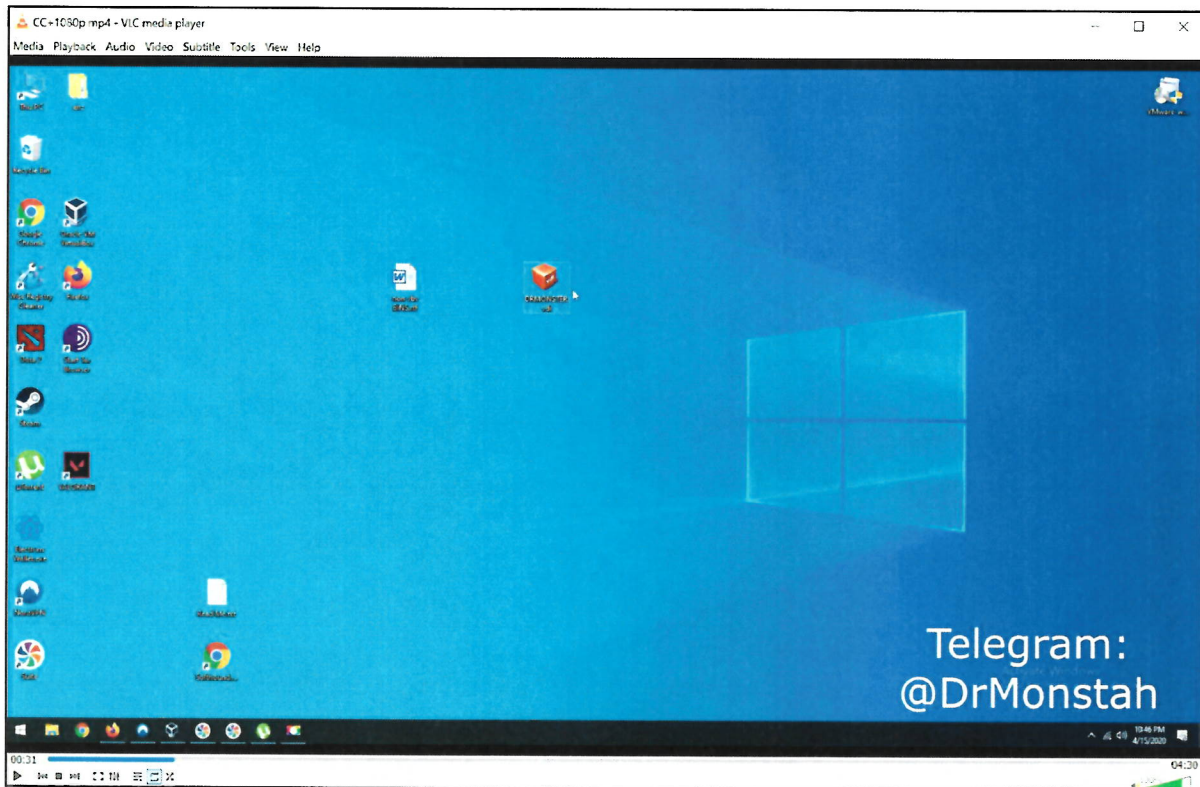
50. EMAIL ACCOUNT 1 received a subsequent email message from Vimeo, dated April 15, 2020 at approximately 11:48 PM, that stated their video, entitled “CC,” was ready to watch on Vimeo. The email included the hyperlink <https://vimeo.com/408251090> (“VIDEO URL 1”) and stated underneath the hyperlink “Only people with a password”. In my training and experience, I know that “CC” is often used as an abbreviation for credit card.

51. On April 10, 2023, the Honorable Michael J. Roemer, U.S. Magistrate Judge of the United States District Court for the Western District of New York, signed a federal search warrant authorizing the FBI to review and download the video stored at VIDEO URL 1.

52. On April 10, 2023, the FBI executed the search warrant for VIDEO URL 1. Agents entered the video password “drmonster” (which agents guessed), after which the video began to play. The video, which is described in detail below, contained a narration (voiced by someone whom agents believe to be CISZEK) and showed the narrator using a “virtual machine” called “DRMONSTER,” while also describing the use of a dark web carding website to purchase credit cards.

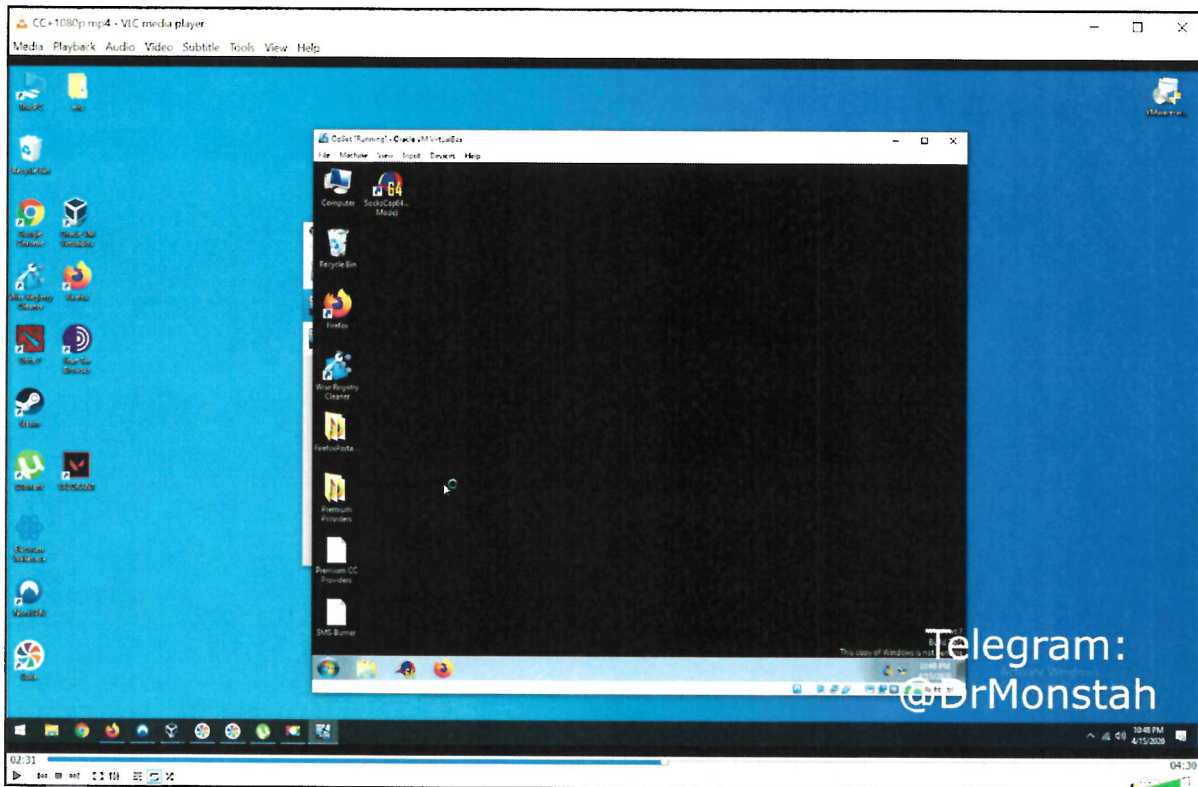
53. The video showed the use of Oracle VirtualBox, SOCKS proxies, and UniCC with narration.¹⁶ The Telegram username @DrMonstah was shown in the lower right corner of the screen during the video. An icon named “DRMONSTER.vdi” was shown on the computer desktop. DRMONSTER is the username of the Genesis Market user who was identified as CISZEK. A VDI file is a virtual machine disk image used by the Oracle VirtualBox desktop virtualization program. A virtual machine, or VM, is a virtual environment that functions as a virtual computer system with its own processor, memory, network interface and storage. A screenshot of the video showing “DRMONSTER.vdi” on the computer desktop is below.

¹⁶ Coinbase records for CISZEK’s Coinbase account showed that on April 13, 2020, CISZEK’s Coinbase account sent 0.02697099 bitcoin to a bitcoin wallet address whose subsequent outbound transfers were limited to bitcoin wallet addresses associated with UniCC and LuxSocks.ru.



54. At approximately 2 minutes and 31 seconds in the video, the virtual machine image DRMONSTER.vdi is loaded in Oracle VirtualBox and booted. A Microsoft Windows 7 Ultimate desktop is loaded with desktop icons that include “Wise Registry Cleaner”, “FirefoxPorta...”, “Premium Providers”, “Premium CC Providers”, “SMS-Burner” and “SockssCap64(Administrator Mode)”. A screenshot of the DRMONSTER.vdi virtual machine image running within Oracle VirtualBox from the video is shown below.¹⁷

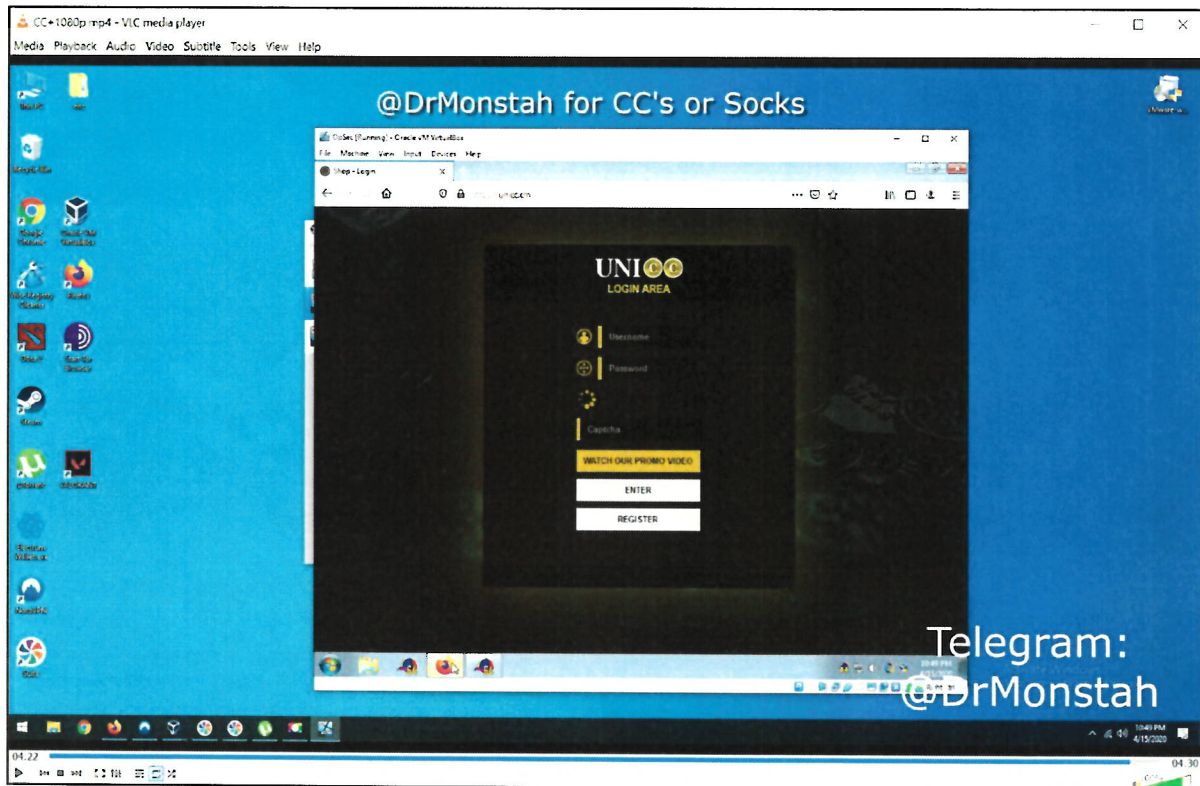
¹⁷ Oracle VirtualBox is desktop-based virtualization software that runs a virtual machine within the user’s computer desktop environment. In the provided screenshot from the video, the DRMONSTER.vdi virtual machine image contained a Microsoft Windows 7 virtual machine that is run within Oracle Virtualbox on a Microsoft Windows 10 computer system.



55. Investigators found a DRMONSTER.vdi virtual machine image file on USB DRIVE 1. Review of the DRMONSTER.vdi virtual machine image file found the desktop icons, “Premium Providers” and “SocksCap64(Administrator Mode)”, in the Administrator user’s Desktop file directory.

56. At approximately 4 minutes and 06 seconds in the video, the narrator states “And then I usually get my credit cards from UniCC which is an amazing place if you guys don’t have it. And I usually get my socks from LuxSocks. And just do your thing. That’s pretty much it. You guys got any questions just text me.” Agents assessed the video narrator’s voice to be

CISZEK's.¹⁸ A screenshot of the video showing the website UniCC loaded on the computer in the video is below.



Web Browser Activity

57. As described below, investigators found other Genesis-related evidence on CISZEK's devices.

¹⁸ Agents' assessment that the video narrator's voice is CISZEK's was based on (1) a review of the video by agents who interviewed CISZEK over the course of approximately 30 minutes on April 4, 2023; (2) a video recording of a police interview, found on USB DRIVE 1, which showed an individual with the same physical likeness as CISZEK, who wore a Buffalo Police jacket, while speaking with a handcuffed individual.

58. The Genesis Market data for DRMONSTER showed that on July 29, 2020 at 1:47:27 (timezone unknown), DRMONSTER accessed Genesis Market from the IP address 107.175.104.236 and downloaded Genesis Market's proprietary web browser.¹⁹ Specifically, DRMONSTER downloaded the files "genesium_browser_19.0_windows32.zip" at 01:46:49 (timezone unknown) and 01:48:06 (timezone unknown) and "genesium_browser_19.0_windows64.zip" at 1:58:33 (timezone unknown) from Genesis Market. Genesium Browser was a propriety web browser that Genesis Market offered its users.

59. Agents' review of the Microsoft Edge web browser history on COMPUTER 1 showed an access to the website address "http://genesis.market/" on July 28, 2020 at 9:45:49 PM -0400. Agents' review of shell bags on COMPUTER 1 found the file "genesium_browser_19.0_windows32.zip" was located in the Downloads directory with the creation date July 29, 2020 01:48:40 UTC.²⁰

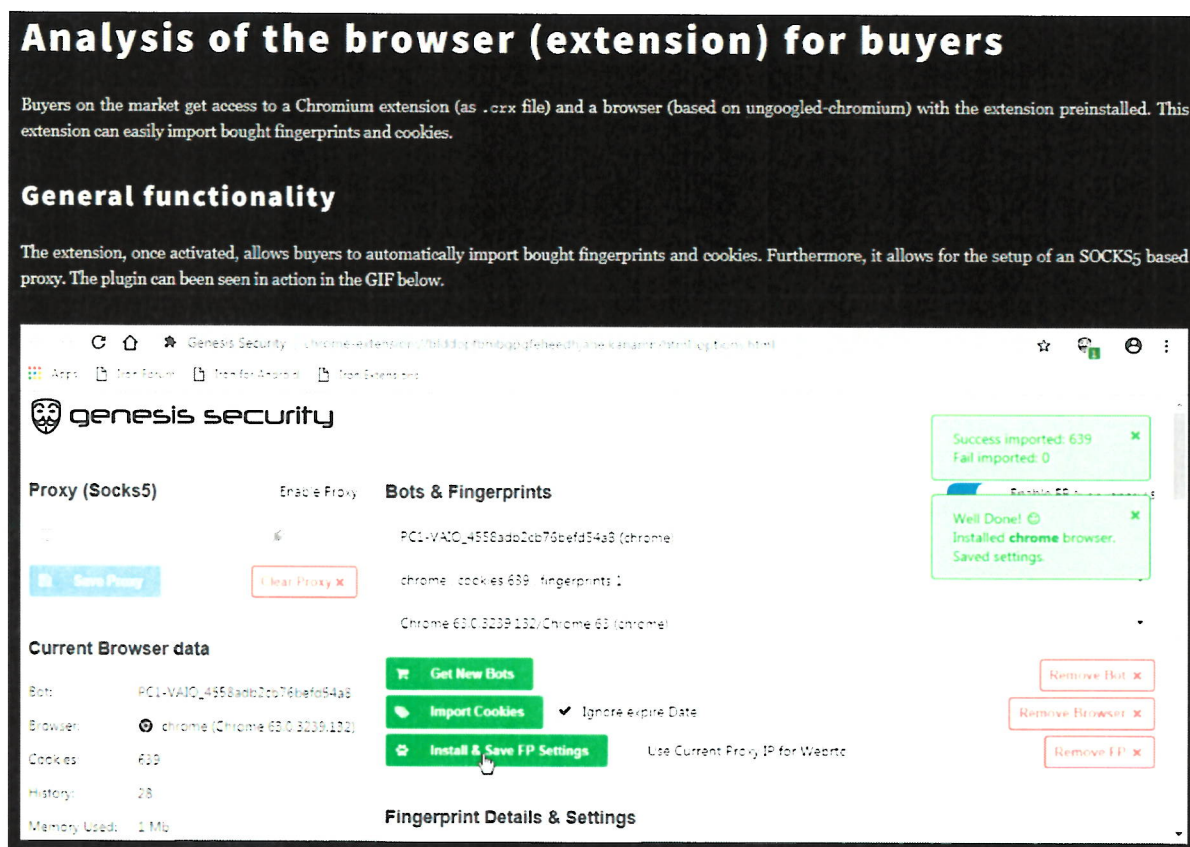
60. Agents' review of COMPUTER 1 found a Google Chrome browser extension with the Chrome Extension ID "blldopfbnibgpgfehedhjaheikanamn" added to a Chromium web browser.²¹

¹⁹ Research found the IP address 107.175.104.236 was associated with the Nord VPN service. A desktop icon for the Nord VPN software appeared on the desktop of the computer depicted in the video from the aforementioned video screenshots.

²⁰ Shell bags are a Microsoft Windows feature used to improve user experience by remembering the user's preferences while the user browses folders on the computer system. For example, when the Microsoft Windows user opens, closes or changes a viewing option of any folder on the computer, a shell bag record is created or updated.

²¹ Chromium is a free and open source web browser project, mainly developed and maintained by Google, that the Google Chrome web browser is built on. Chrome Extension IDs are 32 characters long and uniquely assigned to an extension when signed by Google.

61. On April 5, 2023, Sector7, the research division of Computest, a software development and IT operations company, published a technical analysis article on Genesis Market in which Sector7 stated it had assisted Dutch police in investigating Genesis Market for several weeks.²² Sector7's article discussed how buyers on Genesis Market received access to a Chromium extension that could easily import bought fingerprints and cookies. Sector7's article included a screenshot of the Genesis Market browser extension, which is included below.



²² See Sector7, *Technical analysis of the Genesis Market*, April 5, 2023, available at <https://sector7.comptest.nl/post/2023-04-technical-analysis-genesis-market/> (last visited April 24, 2023).

62. Chromium will show a browser extensions' Chrome Extension ID in the address bar when that browser extension is loaded. Sector7's screenshot showed the Genesis Market browser extension, named Genesis Security, had the Chrome Extension ID "blddopfbnibgpgfeheedhjaheikanamn".

63. These facts provide probable cause that CISZEK, the user of COMPUTER 1, accessed Genesis Market at the same time that the Genesis Market user DRMONSTER downloaded the Genesium Browser from Genesis Market.

CONCLUSION

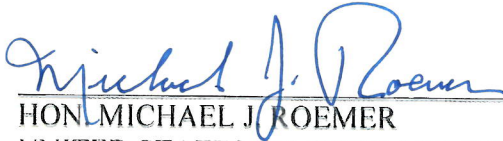
64. Based on the foregoing, I respectfully submit that there is probable cause to believe that TERRANCE MICHAEL CISZEK did violate Title 18, United States Code, Section 1029(a)(3) (knowingly and with intent to defraud, possessing fifteen or more devices which are counterfeit or unauthorized access devices). I respectfully request that the Court issue the attached criminal complaint, as well as an arrest warrant. To allow the warrant to be effectuated, I respectfully request that the criminal complaint, this affidavit, and the arrest warrant remain under seal.

Respectfully submitted,



Bryan Scheiber
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on Apr. 1 27, 2023



HON. MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE